

Dec 07, 2023

s/ Mariah Kauder

Deputy Clerk, U.S. District Court  
Eastern District of Wisconsin

## UNITED STATES DISTRICT COURT

for the

Eastern District of Wisconsin

In the Matter of the Search of )

(Briefly describe the property to be searched )

or identify the person by name and address) )

information associated with a certain cellular telephone assigned call  
number 816-389-7550 ("the SUBJECT PHONE") that is stored at premises  
controlled by AT&T, a wireless telephone service provider headquartered at  
11760 US Highway 1, Suite 300, North Palm Beach, Florida, 33408. )

Case No. 23-M-503 (SCD)

## WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search and seizure  
of the following person or property located in the Eastern District of Wisconsin

(identify the person or describe the property to be searched and give its location):

Please see Attachment A.

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property  
described above, and that such search will reveal (identify the person or describe the property to be seized):

Please see Attachment B.


YOU ARE COMMANDED to execute this warrant on or before 12-21-23 (not to exceed 14 days)

☐ in the daytime 6:00 a.m. to 10:00 p.m. ☒ at any time in the day or night because good cause has been established.Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the  
person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the  
property was taken.The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory  
as required by law and promptly return this warrant and inventory to Honorable Stephen C. Dries

(United States Magistrate Judge)

☐ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C.  
§ 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose  
property, will be searched or seized (check the appropriate box)☐ for days (not to exceed 30) ☐ until, the facts justifying, the later specific date of

Date and time issued: 12-7-23 10:00 am

  
Judge's signature

City and state: Milwaukee, WI

Honorable Stephen C. Dries, U.S. Magistrate Judge

Printed name and title

<b>Return</b>		
Case No.:	Date and time warrant executed:	Copy of warrant and inventory left with:
Inventory made in the presence of :		
Inventory of the property taken and name(s) of any person(s) seized:		
<b>Certification</b>		
<p>I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.</p> <div style="display: flex; justify-content: space-between;"> <div style="width: 30%;"> <p>Date: _____</p> </div> <div style="width: 65%;"> <p style="text-align: center;">_____</p> <p style="text-align: center;"><i>Executing officer's signature</i></p> <p style="text-align: center;">_____</p> <p style="text-align: center;"><i>Printed name and title</i></p> </div> </div>		

## **ATTACHMENT A**

### **Property to Be Searched**

This warrant applies to records and information associated with the cellular telephone assigned call number **816-389-7550** (“the Account”) that are stored at premises controlled by AT&T (“the Provider”), headquartered at 11760 US Highway 1, Suite 300, North Palm Beach, Florida, 33408.

## **ATTACHMENT B**

### **Particular Things to be Seized**

#### **I. Information to be Disclosed by the Provider**

To the extent that the information described in Attachment A is within the possession, custody, or control of the Provider, including any information that has been deleted but is still available to the Provider or that has been preserved pursuant to a request made under 18 U.S.C. § 2703(f), the Provider is required to disclose to the government the following information pertaining to the Accounts listed in Attachment A for the time periods from August 28, 2023, through November 10, 2023:

- a. The following information about the customers or subscribers of the Accounts:
  - i. Names (including subscriber names, usernames, and screen names);
  - ii. Addresses (including mailing addresses, residential addresses, business addresses, and e-mail addresses);
  - iii. Local and long-distance telephone connection records;
  - iv. Records of session times and durations, and the temporarily assigned network addresses (such as Internet Protocol (“IP”) addresses) associated with those sessions;
  - v. Length of service (including start date) and types of service utilized;
  - vi. Telephone or instrument numbers (including MAC addresses, Electronic Serial Numbers (“ESN”), Mobile Electronic Identity Numbers (“MEIN”), Mobile Equipment Identifier (“MEID”); Mobile Identification Number (“MIN”), Subscriber Identity Modules (“SIM”), Mobile Subscriber Integrated Services Digital Network Number (“MSISDN”); International Mobile Subscriber Identity Identifiers (“IMSI”), or International Mobile Equipment Identities (“IMEI”);
  - vii. Other subscriber numbers or identities (including the registration Internet Protocol (“IP”) address); and

- viii. Means and source of payment for such service (including any credit card or bank account number) and billing records.
- b. All records and other information (not including the contents of communications) relating to wire and electronic communications sent or received by the Accounts, including:
  - i. Records of user activity for each connection made to or from the Accounts, including log files; text messaging logs; the date, time, length, and method of connections; data transfer volume; usernames; and source and destination Internet Protocol addresses;
  - ii. Information about each communication sent or received by the Accounts, including the date and time of the communication, the method of communication, and the source and destination of the communication (such as the source and destination telephone numbers, email addresses, and IP addresses); and
  - iii. All data regarding the cell tower and antenna face (also known as “sectors”) through which the communications were sent and received;
  - iv. All historical GPS or other precision location information associated with each Accounts listed in Attachment A, including Per Call Measurement Data (PCMD), Range to Tower/Real-Time Tool (RTT) data, NELOS records, and Timing Advance Data (TrueCall)).

## **II. Information to be Seized by the Government**

All information described above in Section I that constitutes evidence of violations of 18 U.S.C. § 2251(a), 18 U.S.C. § 2252A(a)(1) and 2252A(b)(1), 18 U.S.C. § 2252A(a)(1) and 2252A(b)2, 18 U.S.C. § 2422(a), and 18 U.S.C. § 2423(a), during the period from August 28, 2023, through November 10, 2023.

Dec 07, 2023

s/ Mariah Kauder

Deputy Clerk, U.S. District Court  
Eastern District of Wisconsin

## UNITED STATES DISTRICT COURT

for the  
Eastern District of Wisconsin

## In the Matter of the Search of

(Briefly describe the property to be searched  
or identify the person by name and address)information associated with a certain cellular telephone assigned call  
number 816-389-7550 ("the SUBJECT PHONE") that is stored at premises  
controlled by AT&T, a wireless telephone service provider headquartered at  
11760 US Highway 1, Suite 300, North Palm Beach, Florida, 33408.

Case No. 23-M-503 (SCD)

## APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under  
penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the  
property to be searched and give its location):

Please see Attachment A.

located in the Eastern District of Wisconsin, there is now concealed (identify the  
person or describe the property to be seized):

Please see Attachment B.

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	Offense Description
18 U.S.C. § 2251(a) - Production of Child Pornography, 18 U.S.C. § 2252A(a)(1) and 2252A(b)(1) - Transportation of Child Pornography, 18 U.S.C. § 2252A(a)(1) and 2252A(b)(2) - Possession of Child Pornography, 18 U.S.C. § 2422(a) - Coercion and Enticement of Minors, and 18 U.S.C. § 2423(a) - Transportation of Minors	

The application is based on these facts:

Please see Affidavit.

- ☒ Continued on the attached sheet.
- ☐ Delayed notice of \_\_\_\_\_ days (give exact ending date if more than 30 days: \_\_\_\_\_) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.



Applicant's signature

Daniel Gartland, Special Agent, FBI

Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by  
telephone (specify reliable electronic means).

Date: 12-7-23



Judge's signature

City and state: Milwaukee, WI

Honorable Stephen C. Dries, U.S. Magistrate Judge

Printed name and title

**AFFIDAVIT IN SUPPORT OF**  
**AN APPLICATION FOR A SEARCH WARRANT**

I, Daniel Gartland, being first duly sworn on oath, on information and belief state:

**I. INTRODUCTION, BACKGROUND, TRAINING, AND EXPERIENCE:**

1. I make this affidavit in support of an application for a search warrant for information associated with a certain cellular telephone assigned call number **816-389-7550** ("the SUBJECT PHONE") that is stored at premises controlled by AT&T, a wireless telephone service provider headquartered at 11760 US Highway 1, Suite 300, North Palm Beach, Florida, 33408. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. § 2703(c)(1)(A) to require AT&T to disclose to the government copies of the information further described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review the information to locate items described in Section II of Attachment B.

2. I am a Special Agent (SA) with the Federal Bureau of Investigation (FBI) and have been so employed since May 2018. As such, I am a "federal law enforcement officer" within the meaning of Federal Rule of Criminal Procedure 41(a)(2)(C), that is, a government agent engaged in enforcing the criminal laws and duly authorized by the Attorney General to request search and arrest warrants. I am currently assigned to the FBI Milwaukee Division and am a member of the Milwaukee Child Exploitation and Human Trafficking Task Force. I am authorized to investigate violent crimes against children, to include the enticement or kidnapping of children, the possession, production, and distribution of child sexual abuse material (commonly known as "CSAM").

3. I have received training related to the investigation and enforcement of federal child pornography and child exploitation laws. As a result of this training and my experience, I am familiar with the methods by which electronic devices are used as the means for receiving, transmitting, possessing, and distributing images and videos depicting minors engaged in sexually explicit conduct (hereafter referred to as "child pornography"). I have also received training and gained experience in interviewing and interrogation techniques, arrest procedures, search warrant applications, the execution of searches and seizures, electronic device evidence identification, electronic device evidence seizure and processing, and various other criminal laws and procedures.

4. Based on the facts set forth in this affidavit, there is probable cause that the cellular device with telephone number **816-389-7550** contains evidence and/or instrumentalities of violations of 18 U.S.C. § 2251(a), 18 U.S.C. § 2252A(a)(1) and 2252A(b)(1), 18 U.S.C. § 2252A(a)(1) and 2252A(b)(2), 18 U.S.C. § 2422(a), and 18 U.S.C. § 2423(a), as described in Attachment B.

5. This affidavit is based upon my training and experience, my personal knowledge and information reported to me by other federal, state, and local law enforcement officers during the course of their official duties, all of whom I believe to be truthful and reliable. This affidavit is also based upon police reports, forensic analysis of digital devices, open-source information, reports from Electronic Service Providers, and subject interviews that I consider to be reliable as set forth herein.

6. Because this affidavit is submitted for the limited purpose of obtaining a search warrant, I have not included each and every fact known to me concerning this investigation.



## II. DEFINITIONS

7. The following definitions apply to the Affidavit and Attachments A and B to this Affidavit:

a. “Cellular telephone” or “cell phone” means a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional “land line” telephones. A wireless telephone usually contains a “call log,” which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic “address books”; sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may include geolocation information indicating where the cell phone was at particular times.

b. “Child Pornography” is defined in 18 U.S.C. § 2256(8) as any visual depiction of sexually explicit conduct where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct, (b) the visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct, or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct.

c. “Computer” is defined pursuant to 18 U.S.C. § 1030(e)(1) as “an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device.”

d. “Computer Server” or “Server,” is a computer that is attached to a dedicated network and serves many users. A web server, for example, is a computer that hosts the data associated with a website. That web server receives requests from a user and delivers information from the server to the user’s computer via the Internet. A domain name system (DNS) server, in essence, is a computer on the Internet that routes communications when a user types a domain name, such as www.cnn.com, into his or her web browser. Essentially, the domain name must be translated into an Internet Protocol (IP) address so the computer hosting the web site may be located, and the DNS server provides this function.

e. “Computer hardware” means all equipment which can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data-processing devices (including, but not limited to, central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, and other memory storage devices); peripheral input/output devices (including, but not limited to, keyboards, printers, video display monitors, and related communications devices such as cables and connections), as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including, but not limited to, physical keys and locks).

f. “Computer software” is digital information which can be interpreted by a computer and any of its related components to direct the way they work. Computer software is

stored in electronic, magnetic, or other digital form. It commonly includes programs to run operating systems, applications, and utilities.

g. “Computer-related documentation” consists of written, recorded, printed, or electronically stored material which explains or illustrates how to configure or use computer hardware, computer software, or other related items.

h. “Computer passwords, pass phrases and data security devices” consist of information or items designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password or pass phrase (a string of alpha-numeric characters) usually operates as a sort of digital key to “unlock” particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software of digital code may include programming code that creates “test” keys or “hot” keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or “booby-trap” protected data to make it inaccessible or unusable, as well as reverse the process to restore it.

i. “Electronic storage devices” includes computers, cellular telephones, tablets, and devices designed specifically to store electronic information (e.g., external hard drives and USB “thumb drives”). Many of these devices also permit users to communicate electronic information through the internet or through the cellular telephone network (e.g., computers, cellular telephones, and tablet devices such as an iPad).

j. The “Internet” is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between

devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

k. “Internet Service Providers” (ISPs) are commercial organizations that are in business to provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers including access to the Internet, web hosting, e-mail, remote storage, and co-location of computers and other communications equipment. ISPs can offer a range of options in providing access to the Internet including telephone-based dial-up, broadband based access via digital subscriber line (DSL) or cable television, dedicated circuits, or satellite based subscription. ISPs typically charge a fee based upon the type of connection and volume of data, called bandwidth, which the connection supports. Many ISPs assign each subscriber an account name – a username or screen name, an “e-mail address,” an e-mail mailbox, and a personal password selected by the subscriber. By using a computer equipped with a modem, the subscriber can establish communication with an Internet Service Provider (ISP) over a telephone line, through a cable system or via satellite, and can access the Internet by using his or her account name and personal password.

l. “An Internet Protocol address” (IP address) is a unique numeric address used by internet-enabled electronic storage devices to access the Internet. An IP address is a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every electronic storage device attached to the Internet must be assigned an IP address so that Internet traffic sent from and directed to that electronic storage device may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static, that is, long-term IP addresses, while other computers have dynamic that is, frequently changed IP addresses.

m. “Hash Value” refers to the process of using a mathematical function, often called an algorithm, to generate a numerical identifier for data. A hash value can be thought of as a “digital fingerprint” for data. If the data is changed, even very slightly (like the addition or deletion of a comma or a period), the hash value changes. Therefore, if a file such as a digital photo is a hash value match to a known file, it means that the digital photo is an exact copy of the known file.

n. “Media Access Control” (MAC) address means a hardware identification number that uniquely identifies each device on a network. The equipment that connects a computer to a network is commonly referred to as a network adapter. Most network adapters have a MAC address assigned by the manufacturer of the adapter that is designed to be a unique identifying number. A unique MAC address allows for proper routing of communications on a network. Because the MAC address does not change and is intended to be unique, a MAC address can allow law enforcement to identify whether communications sent or received at different times are associated with the same adapter.

o. “Minor” means any person under the age of eighteen years. See 18 U.S.C. § 2256(1).

p. The terms “records,” “documents,” and “materials” include all information recorded in any form, visual or aural, and by any means, whether in handmade form (including writings and drawings), photographic form (including prints, negatives, videotapes, motion pictures, and photocopies), mechanical form (including printing and typing) or electrical, electronic or magnetic form (including tape recordings, compact discs, electronic or magnetic storage devices such as hard disks, CD-ROMs, digital video disks (DVDs), Personal Digital Assistants (PDAs), Multi Media Cards (MMCs), memory sticks, smart cards, or electronic

notebooks, as well as digital data files and printouts or readouts from any magnetic, electrical or electronic storage device).

q. “Sexually explicit conduct” means actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the genitals or pubic area of any person. See 18 U.S.C. § 2256(2).

r. “Visual depictions” include undeveloped film and videotape, and data stored on computer disk or by electronic means, which is capable of conversion into a visual image. See 18 U.S.C. § 2256(5).

### **III. PROBABLE CAUSE**

8. On November 4, 2023, The Kenosha County Sheriff’s Department (KCSO) received a complaint from Julie White. She reported that when she awoke at approximately 7:30 a.m., her niece A.E., a 15-year-old minor, was missing from her apartment at 34502 Geneva Road, Burlington, WI. A.E. had stayed with White, while A.E.’s parents were out of town.

9. White fell asleep at approximately 2:00 a.m., after seeing A.E. enter the bathroom of the residence. When White awoke, the bathroom door was still closed, but A.E. was not present. White observed that the bathroom window was closed, but the screen was on the ground outside of the window. White believed A.E. did not have a phone and she could not locate her.

10. A.E. was last seen wearing a black hooded sweatshirt, black leggings, and black and white Nike shoes. A red Christmas blanket was missing from White’s residence and was believed to be with A.E.

11. Surveillance video from that night was obtained from businesses in close proximity to White’s apartment building, including Honeydripperz Pub at 34500 Geneva Road, Burlington,

WI. The video depicted a silver sedan park in the area of White's apartment at approximately 2:10 a.m. The video depicted a black male appear, consistent with arriving with the vehicle. The black male was wearing dark colored shoes, light colored pants and long dark coat. He walked around in the area of White's apartment building, then returned to the area where the sedan was parked. The sedan then departed.

12. A law enforcement officer from the KCSD interviewed an employee of Honeydripperz Pub on November 7, 2023. The employee departed Honeydripperz Pub while the sedan was still parked in the area. She noted that the sedan had a light up Uber sign.

13. A search warrant was obtained in Kenosha County District Court for devices with Google accounts located in a small geographic area encompassing the location where the sedan parked. Data provided by Google in response to the warrant included Google Subscriber information for Shofu Rahman. A search of law enforcement databases revealed that Rahman resided in Milwaukee, WI. A silver 2013 Hyundai Accent sedan was registered to Rahman.

14. KCSD detectives interviewed Rahman at his home. He stated that he was a driver for both the Uber and Lyft rideshare services. He typically conducted rideshares from the Milwaukee Airport.

15. Rahman allowed KCSD Detectives to review his rideshare applications on his phone. The Lyft application showed that Rahman accepted a rideshare at approximately 12:55 a.m. on November 4, 2023. Rahman drove a passenger from Milwaukee to Burlington, WI, arriving at approximately 2:01 a.m. Rahman was stopped at the location for approximately 15 minutes. Rahman then drove the passenger to back to Milwaukee, arriving at 3:12 a.m.

16. The passenger told Rahman that he was looking for a person in Burlington. When he could not find the person, Rahman drove him to the Milwaukee Intermodal Station. Upon

arriving at the station, the passenger asked Rahman to take him back to Burlington. Rahman stated the passenger's name was "Said."

17. Surveillance video obtained from the Milwaukee Intermodal Tran Station from that same night, located at 433 West St. Paul Avenue, Milwaukee, WI, depicted a black male with a long black coat and dreadlocks enter the building at the approximate time Rahman dropped off his passenger. The individual was observed using his cellular telephone multiple times within the building. At approximately 4:19 a.m., the individual exited the building. At 4:20 a.m., he walked back into the building with a small, white female, wearing a black hooded sweatshirt with the hood up and black pants. The female was carrying a red blanket. Detectives identified the white female as A.E.

18. KCSD detectives conducted a search of A.E.'s home and bedroom with the consent of her mother. Detectives observed drawings with the name "Liam" written on them in A.E.'s bedroom. They also observed a receipt for the food delivery service DoorDash on October 22, 2023. The receipt included customer name "Anna E" and order number "d5a3e2cf-ce".

19. On November 9, 2023, DoorDash, Inc. responded to an exigent request for information regarding DoorDash order number d5a3e2cf-ce. The information provided identified A.E. as the customer. The phone number associated with the order was **816-389-7550**. The email address associated with the order was kaidawhite03@gmail.com. The order was paid for via a Visa credit card with the last four digits of 9160.

20. KCSD detectives also located a daily planner in one of A.E.'s backpacks. The word "Liam" was written in the planner on November 3, 2023. A heart was drawn around the name. The phrase "out of state" was also written in the planner near November 3, 2023.

21. KCSD detectives interviewed A.E.'s minor friend S.F. in the presence of S.F.'s



parents. S.F. knew A.E. to be communicating with older males online. S.F. knew one of the older males A.E. talked to was named “David.” S.F. knew A.E.’s Snapchat account name to be, “Lunny\_toons420”.

22. KCSD detectives interviewed A.E.’s minor friend B.L. in the presence of B.L.’s mother. B.L. knew A.E. communicated with older men via Instagram and Snapchat. A.E. told B.L. that one of the people A.E. was speaking to could help her get away from her family. Approximately one week prior to A.E.’s disappearance, A.E. told B.L. that she planned to run away to Maryland.

23. KCSD detectives interviewed A.E.’s minor friend A.V. in the presence of A.V.’s parents. A.E. told A.V. that she met a male online who had a wife and son her age and that they offered to take A.E. into their home. The person A.E. met online lived in Maryland and the son was African American. A.E. talked about the name “Liam.” A.V. was unsure if it was the name of the person A.E. was talking to or the son. A.E. told A.V. the husband was going to fly to Milwaukee, Anna was going to meet him there, and they would ride back to Maryland together. A.E. told A.V. the man had given her his credit card to order food from DoorDash.

24. A.V. told detectives that A.E. had a phone that she kept hidden from her parents. A.V. received a message via Snapchat from A.E. on November 4, 2023. The message stated that A.E. was in Milwaukee and that she loved her. A.V. believed A.E. planned to destroy her phone and discontinue contact with her friends for three months.

25. A search warrant was obtained in Kenosha County District Court for A.E.’s Snapchat account, “Lunny\_tunes420”. Snapchat provided information in response to the search warrant on November 9, 2023. Detectives observed the date of birth for the account owner to be the same as A.E.’s date of birth. The information also indicated the account was last active on

November 4, 2023.

26. Detectives observed that A.E. added Snapchat account “liaminca” as a friend on August 28, 2023. The same user was removed as a friend on November 6, 2023. Portions of communications between A.E. and Snapchat user “liaminca” were provided by Snapchat in response to the search warrant. Detectives observed images of lingerie, underwear and bras that “liaminca” sent to A.E. Based upon my training and experience, I know individuals that send images of lingerie and undergarments to minors, will often entice those minors to progressively produce images of themselves in lingerie, nude or sexual images of themselves. Those individuals then retain those images on phones or in other electronic storage devices.

27. They also observed a satellite image sent from A.E. to “liaminca”. The image included A.E.’s residence at 34517 Geneva Road, Burlington, WI, which was marked, “where I live.” A red line from A.E.’s residence to a black dot were overlayed onto the image. The red line included the text, “way I’ll take” and the black dot included the text, “where we meet.” The words, “where you park” overlayed the parking lot at Best Bargains, 6515 352<sup>nd</sup> Avenue, Burlington, WI, 53105.

28. Detectives observed the avatar of the “liaminca” Snapchat account was a black male with dreadlocks. An open-source search of multiple social media platforms was conducted for account names similar to “liaminca”. The username “liaminca” was located on the Kik messaging platform. The profile image associated with the account was a black male with dreadlocks. The image was consistent with the black male observed on surveillance video in the area of White’s apartment building.

29. Detectives submitted the profile photo of Kik user “liaminca” to the Mid-States Organized Crime Information Center (MOCIC). MOCIC used facial recognition software to

identify a photo associated with the Facebook account “Blaise Dk”. Detectives reviewed posts associated with the account. The Facebook page “Mina Abdussabur” posted a photo of the same black male with the caption, “Because I have a Black Son”.

30. A search of law enforcement databases produced a result for a Mina Abdussabur with ties to Baltimore, Maryland. Abdussabur also had potential relatives by the names of Said A Hamza, Said Hussain Hamza, and Said Mukhtaar Hamza.

31. A search of law enforcement databases was conducted for information related to Said Mukhtaar Hamza (XX/XX/1994). He was associated telephone number **816-389-7550**, the same number associated with the DoorDash order receipt recovered from A.E.’s bedroom. Hamza was also associated with several addresses in Baltimore, Maryland.

32. Information was requested from the Greyhound Bus Lines for any tickets purchased by Said Mukhtaar Hamza on November 4, 2023. Greyhound Bus Lines provided ticket information for two passengers, “Said Hamza” and “Anna Estesa”. The tickets departed the Milwaukee Bus Station, 433 West St. Paul Avenue, Milwaukee, WI, at 6:40 a.m. on November 4, 2023 and arrived in Baltimore, Maryland on November 5, 2023 at approximately 8:25 p.m.

33. KCSD Detectives issued a temporary felony warrant for Said Mukhtaar Hamza for violations of Wisconsin state statutes 940.31(1)(c), Felony Kidnapping, and 948.30(1)(a), Felony Abduction of a Child.

34. An exigent request for information was submitted to AT&T Wireless for Timing Advanced Data records for telephone number **816-389-7550** for November 4, 2023. An analysis of the records revealed the telephone was located at the Milwaukee Mitchell International Airport at approximately 1:00 a.m. on November 4, 2023. The phone then traveled to an area near Julie White’s residence in Burlington, WI, arriving at approximately 2:20 a.m. The device then returned

to an area encompassing the Milwaukee Intermodal Station, arriving at approximately 3:10 a.m. The device departed the area at approximately 7:17 a.m., moving in a direction consistent with travel along U.S. Interstate 43 and U.S. Interstate 94.

35. KCSD Detectives contacted the Baltimore Police Department for assistance in recovering A.E. and arresting Said Mukhtar Hamza.

36. KCSD Detectives obtained a search warrant in Kenosha County District Court for the Snapchat account “liaminca”. Snapchat provided information in response to the search warrant on November 9, 2023. Detectives observed the date of birth for the account owner to have the same month and day as Hamza with a different birth year of 2005. The phone number associated with the account was **816-319-7550**. Detectives observed multiple selfie-style images associated with the account. Based upon my training and experience, I believe Hamza used an incorrect birth year when establishing his Snapchat account to imply a younger age when communicating with minors via Snapchat.

37. Detectives observed a photo from November 5, 2023 which depicted A.E. and Said Mukhtar Hamza on a bus. Communications between “liaminca” and A.E. were included in the records provided by Snapchat. One such communication appeared to discuss age, but only included A.E.’s messages. A.E. stated, “15,” followed by a question regarding liaminca’s age. A.E. then stated, “You don’t look 25, I thought you were 16.”

38. The Snapchat records included communications between “liaminca” and other Snapchat users. During one such communication with a user believed to be from Austria, liaminca stated, I’ve never been but you look like a good reason to visit.....You laugh but I’d kidnap you frfr.”

39. On November 10, 2023, Said Mukhtar Hamza was taken into custody by the

Baltimore Police Department at 3912 10<sup>th</sup> Street, Baltimore Maryland. A.E. was located within the residence, unclothed. Detectives observed that A.E. appeared to have hematomas, more commonly referred to as “hickeys,” on her neck.

40. On November 10, 2023, a Baltimore Police Detective conducted a custodial interview of Said Mukhtar Hamza. After being advised of his Miranda rights and waiving those rights, Hamza agreed to speak with the Detective. Hamza stated that he met A.E. through an online dating application several months prior. Hamza and A.E. made a plan for her to come to Baltimore. Hamza traveled to Wisconsin, transported A.E. away from her home using a ride share application, then traveled with her via bus to Baltimore. Hamza stated that, once in Baltimore, he engaged in sexual intercourse with A.E. an unknown number of times.

41. On November 10, 2023, the Baltimore Police Department executed a search warrant at 3912 10<sup>th</sup> Street. During the search, the following items were located in a bedroom believed to belong to Hamza:

- Two Dell laptops,
- Bedding, including one comforter and one sheet,
- Assorted credit cards, and
- One black in color iPhone.

Among the assorted credit cards was a card in the name of Said Hamza. The last four digits of the card were 9160, which matched the last four digits of the card on the DoorDash receipt recovered in A.E.’s bedroom. Hamza’s government identification was also recovered from the room. The iPhone was submitted to the Baltimore Evidence Control Unit under property number 4970008. The two Dell laptops were submitted to the Baltimore Evidence Control Unit under property number 4975235 and property number 4975236.

42. On November 15, 2023, a Baltimore Police Detective obtained a warrant to search the iPhone for evidence of violations of Maryland Criminal Law Code CR 3-324 Sexual Solicitation of Minor, CR-503(a) Kidnapping of a child under 16, and CR3-307 Sex Offense Third Degree. The Baltimore Police Department attempted to execute the warrant by conducting a forensic download of the device. The attempt was not successful, and the device remains in the custody of the Baltimore Police Department. Prior to conducting the forensic download, a manual preview of the device was conducted. Various images of Hamza and A.E. in a bed were observed on the phone. The Federal Bureau of Investigation agreed to conduct a forensic download of the device in support of a federal investigation into the incident. The warrant obtained by the Baltimore Police Department does not contain the appropriate language that would allow federal agents to execute the warrant.

#### **AUTHORIZATION REQUEST**

1. Based on the foregoing, I request that the Court issue the proposed search warrant, pursuant to 18 U.S.C. § 2703(c) and Federal Rule of Criminal Procedure 41.

2. I further request that the Court direct AT&T to disclose to the government any information described in Section I of Attachment B that is within its possession, custody, or control. Because the warrant will be served on AT&T, who will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

## **ATTACHMENT A**

### **Property to Be Searched**

This warrant applies to records and information associated with the cellular telephone assigned call number **816-389-7550** (“the Account”) that are stored at premises controlled by AT&T (“the Provider”), headquartered at 11760 US Highway 1, Suite 300, North Palm Beach, Florida, 33408.

## **ATTACHMENT B**

### **Particular Things to be Seized**

#### **I. Information to be Disclosed by the Provider**

To the extent that the information described in Attachment A is within the possession, custody, or control of the Provider, including any information that has been deleted but is still available to the Provider or that has been preserved pursuant to a request made under 18 U.S.C. § 2703(f), the Provider is required to disclose to the government the following information pertaining to the Accounts listed in Attachment A for the time periods from August 28, 2023, through November 10, 2023:

- a. The following information about the customers or subscribers of the Accounts:
  - i. Names (including subscriber names, usernames, and screen names);
  - ii. Addresses (including mailing addresses, residential addresses, business addresses, and e-mail addresses);
  - iii. Local and long-distance telephone connection records;
  - iv. Records of session times and durations, and the temporarily assigned network addresses (such as Internet Protocol (“IP”) addresses) associated with those sessions;
  - v. Length of service (including start date) and types of service utilized;
  - vi. Telephone or instrument numbers (including MAC addresses, Electronic Serial Numbers (“ESN”), Mobile Electronic Identity Numbers (“MEIN”), Mobile Equipment Identifier (“MEID”); Mobile Identification Number (“MIN”), Subscriber Identity Modules (“SIM”), Mobile Subscriber Integrated Services Digital Network Number (“MSISDN”); International Mobile Subscriber Identity Identifiers (“IMSI”), or International Mobile Equipment Identities (“IMEI”);
  - vii. Other subscriber numbers or identities (including the registration Internet Protocol (“IP”) address); and



- viii. Means and source of payment for such service (including any credit card or bank account number) and billing records.
- b. All records and other information (not including the contents of communications) relating to wire and electronic communications sent or received by the Accounts, including:
  - i. Records of user activity for each connection made to or from the Accounts, including log files; text messaging logs; the date, time, length, and method of connections; data transfer volume; usernames; and source and destination Internet Protocol addresses;
  - ii. Information about each communication sent or received by the Accounts, including the date and time of the communication, the method of communication, and the source and destination of the communication (such as the source and destination telephone numbers, email addresses, and IP addresses); and
  - iii. All data regarding the cell tower and antenna face (also known as “sectors”) through which the communications were sent and received;
  - iv. All historical GPS or other precision location information associated with each Accounts listed in Attachment A, including Per Call Measurement Data (PCMD), Range to Tower/Real-Time Tool (RTT) data, NELOS records, and Timing Advance Data (TrueCall)).

## **II. Information to be Seized by the Government**

All information described above in Section I that constitutes evidence of violations of 18 U.S.C. § 2251(a), 18 U.S.C. § 2252A(a)(1) and 2252A(b)(1), 18 U.S.C. § 2252A(a)(1) and 2252A(b)2, 18 U.S.C. § 2422(a), and 18 U.S.C. § 2423(a), during the period from August 28, 2023, through November 10, 2023.